UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/557,750	10/30/2006	Pekka Nikander	3772-27	2289

23117 7590 03/18/2010

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
THAO, CHHEAN K	
ART UNIT	PAPER NUMBER
2617	
MAIL DATE	DELIVERY MODE
03/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/557,750	NIKANDER ET AL.	
	Examiner	Art Unit	
	CHHEAN THAO	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *23-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *no IDS filed*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

2. At present claims 23-30 are pending.

3. Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 23-30 are rejected under 35 U.SC. 103(a) as being unpatentable over Haverinen (US 20020012433 A1) in view of Ju (US 20030067923 A1)

Regarding claim 23, Haverinen discloses:

Applicant claims a method of securely authenticating subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, the method comprising:

performing a first run of an authentication and key agreement procedure defined for the radio communication network, between a mobile node and an authentication server of the radio communication network, so as to authenticate the mobile node to the radio communication network (*authentication algorithms which are referred to as A3 and A8. These algorithms run on the SIM and in the GSM telecommunications network. These algorithms and a GSM shared secret K.sub.i are known by the SIM and the GSM telecommunications network operator, which typically stores them in an HLR (Home Location Register) of a Mobile services Switching Centre (MSC); In authentication, the GSM telecommunications network operator generates a challenge RAND (128 bits random code used as challenge) that is a 128 bit random code, which is to be used as a challenge, a corresponding 64 bit GSM session key Kc and a 32 bit signed response SRES for verifying the response to the challenge. The 64 bit session GSM session key Kc is generated by the A8 algorithm as A8(K.sub.i,RAND) and the 32 bit long SRES (signed response extension of the system) is generated by the A3(K.sub.i,RAND); the GSM telecommunications network operator sends the RAND to its subscriber (GSM telephone), the RAND is received by the subscriber and the subscriber passes it to the SIM, which reproduces SRES and Kc. Then the SIM responds to the challenge by sending the SRES. The operator receives the SRES and can confirm the identity of the SIM. The GSM telecommunications network operator can also verify that it shares a Kc with the SIM. Then the Kc can then be used to encrypt data traffic over a GSM radio channel. The advantage of this challenge-response mechanism is that Kc never need be sent over the GSM radio channel and thus it cannot be eavesdropped;* therefore, the first run of authentication and key agreement procedure*; Haverinen, para 0169-0170; fig. 1 and para 0173*);

initiating an authentication procedure with a stable forwarding agent of the mobile routing

system (*The MT sends to the FAAA a Network Access Identifier NAI and a protection code MT_RAND (also known in Mobile IP terminology as nonce) generated by the MT. The MT_RAND remains the same during an authentication session and it is meant to hinder replay attacks; Haverinen, para 178; the FAAA sends to the HAAA an initial identification message containing the IMSI or NAI of the MT, and the MT_RAND; Haverinen, para 179; the HAAA retrieves n GSM triplets, each comprising a RAND, a Kc, and a SRES. Then, the HAAA computes the K= H(n*Kc,MT_RAND) for the MT. Here n is an integer greater than or equal to 1, * represents the number of parameters (n*Kc refers to n different Kcs) and H ( ) represents a one-way hash function. The HAAA also computes a value SIGNrand which is calculated from MAC(K,n*RAND,MT_RAND), where MAC denotes a message authentication code. SIGNrand is a cryptographic checksum to verify that the n RANDs really originate from an entity that has access to the K.sub.i (as K is derived from that). The checksum also indicates if the n RANDs indeed are generated during the same authentication session because the MT_RAND changes from one authentication session to another; Haverinen, para 180*) ;

Performing a second run of the authentication and key agreement procedure between the mobile node and the authentication server so as to generate a shared secret (Authentication is carried out using GSM_B and its SIM, SIM_B. *In this case the authentication procedure will be similar to that described above in relation to a basic GSM network (hint: second run of authentication).* Authentication utilizes the K.sub.i which is present on the SIM_B and in the GSM_B; the MIP does not directly access the K.sub.i of the GSM_B, but receives a RAND relating to the SIM_B. This RAND is sent to the MT and the RESP is verified against the RESP that the telecommunications network has produced. Authentication can be further improved by using multiple RANDs in order to generate an authentication key which is more secure than just one

Kc; Haverinen, para 00175-0176; detail re-authentication steps are further describes in paragraphs 0177-0187**)**;

providing the shared secret to the stable forwarding agent, and using the shared secret to authenticate the mobile node to the stable forwarding agent **(***the HAAA sends also the K (shared secret) to the FAAA. Haverinen, para 0186; FIG. 2 shows a shared session key exchange procedure of the system of FIG. 1(para, 177-187)***)**;

sending a public key from the mobile node to the stable forwarding agent (*The MT sends the SIGNsres (*The MT computes a cryptographic checksum SIGNsres=HASH2(K,n*SRES) for the K and the SRESs; para, 183; MT use the public key (K) in it to encrypt the IMSI value sent over in the IDmt payload. The IMSI value is then known only to the MT and the GAGW, and can be also used to authenticate the PAC to the MT; para 332*) to the FAAA. In the MT, the calculation of the K is the same as the calculation of the K in the HAAA; Haverinen, para 0183-0184*) ;

agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured (*The MT includes the SIGNsres in an SRES extension in the next registration request it sends to the MA. The MA sends the SIGNsres to the HAAA, which verifies it and sends an indication to the MA. If the SIGNsres is valid, the HAAA also sends the K to the MA. Now the MA can create/update the security context for the MT; If the MA is the FA, the K could now be distributed to all the foreign agents in the visited domain; Haverinen, para 0193-0194, fig. 1*)**;**

following authentication of the mobile node to the stable forwarding agent, collecting at the stable forwarding agent subscriber contact information from said authentication server (*Authentication is complete and the FAAA and the MT share the K; the FAAA is functionally*

connected to several HAAAs and the FAAA selects the correct HAAA based on the domain part of the user's NAI; Haverinen, para 0187-0188);

using the subscriber contact information to assign a Fully Qualified Domain Name and/or IP address to the mobile node (*The NAI is in form of imsi@sonera.fi (for example "1234567@sonera.fi") or imsi@gsm.org (for example "1234567@gsm.org"); the NAI carries an identity (for example as text or as an identifier number) of the mobile telecommunications network whose subscriber the mobile node is and an identification of the domain of the mobile node; Haverinen, para 165;Authentication is complete and the FAAA and the MT share the K; the FAAA is functionally connected to several HAAAs and the FAAA selects the correct HAAA based on the domain part of the user's NAI, for example "sonera.fi"; the FAAA is configured to communicate with a single HAAA and always sends the message in step 1 to that HAAA; Haverinen, para 0187-0188*);

and updating a subscriber database and DNS server with the Fully Qualified Domain name and/or IP address and the public key provided by the mobile node (*the FAAA is functionally connected to several HAAAs and the FAAA selects the correct HAAA based on the domain part of the user's NAI, for example "sonera.fi"; the FAAA is configured to communicate with a single HAAA and always sends the message in step 1 to that HAAA; the MA can create/update the security context for the MT; Haverinen, para 0187-0193*)

Although Haverinen discloses all of the limitations, Haverinen fails to expressly teach updating a subscriber database and DNS server with the Fully Qualified Domain name and/or IP address. However, the preceding limitation is known in the art and is taught by the Ju reference. Ju teaches a method for accessing a packet data service through an Internet service network by a mobile station having a unique domain name, the method comprises allocating an IP address for

the packet data service to the mobile station; storing the domain name and the allocated IP address matched to the domain name in a DNS server; and providing the packet data service to the mobile station using the IP address matched to the domain name (Ju, para 00013). Therefore, it would have been obvious to one of ordinary skill in the art to modify Haverinen mobility server by including the DNS server in order to store an IP address allocated to the mobile station and a domain name granted to the mobile station by the AAA during accounting set up process of data session for packet service to a mobile station as taught by Ju .

Regarding claim 24, the combination of Haverinen and Ju disclose a method according to claim 23, further comprising:

transporting messages associated with the second run between the stable forwarding agent used by a mobile node and the authentication server via the stable forwarding agent (*The MT sends to the FAAA a Network Access Identifier NAI and a protection code MT_RAND (also known in Mobile IP terminology as nonce) generated by the MT. The MT_RAND remains the same during an authentication session and it is meant to hinder replay attacks; Haverinen, para 178; the FAAA sends to the HAAA an initial identification message containing the IMSI or NAI of the MT, and the MT_RAND (i.e. transporting messages via the FA); Haverinen, para 179*).

Regarding claim 25, the combination of Haverinen and Ju disclose a method according to claim 23, further comprising:

sending session keys, agreed upon during the second run of the authentication procedure, from the authentication server to the stable forwarding agent (*the HAAA sends also the K to the FAAA. Haverinen, para 0186; FIG. 2 shows a shared session key exchange procedure of the system of FIG. 1(para, 177-187)*).

Regarding claim 26, the combination of Haverinen and Ju disclose a method according to claim 23, further wherein the mobile routing system is a Mobile IP based system, and the stable forwarding agent is a Home Agent (*The PAC can also function as a mobility agent MA. If the MIP (i.e. Mobile IP based system) is the home network of the MT, then the PAC is also a Home Agent HA of the MT. Otherwise the PAC belongs to a foreign network and the PAC can be referred to as a Foreign Agent FA; Haverinen, para 174*)**.**

Regarding claim 27, the combination of Haverinen and Ju disclose a method according to claim 23, wherein the mobile routing system is a HIP (Host Identity Protocol, Home Agent is replaced by a Forwarding Agent (or anchor point). It is the Forwarding Agent which acts as the intermediary between the mobile node and the HLR during the AKA re-run) based system (*the packet data network is an IP network. Most preferably, the packet data network is a mobile IP network (i.e. HIP); Haverinen, para 40; If the MIP is the home network of the MT, then the PAC is also a Home Agent HA of the MT. Otherwise the PAC belongs to a foreign network and the PAC can be referred to as a Foreign Agent FA; Haverinen, para 174, fig. 1*).

Regarding claim 28, the combination of Haverinen and Ju disclose a method according to claim 23, wherein said authentication and key agreement procedure is the Authentication and Key Agreement procedure specified by 3GPP (*Subscriber Identity Module is used in generating of the session secret based on a shared secret specific for the mobile node identity; Haverinen, para 30; retrieving the mobile node identity and the shared secret from the mobile station to the mobile node; Haverinen, para 45; therefore, 3GPP procedure*).

Regarding claim 29, the combination of Haverinen and Ju disclose a method according to claim 23, wherein the collected subscriber contact information comprises one or more of the following:

the name and postal address of a subscriber **(***the home GSM network stores customer information, such as authentication codes and user identity; therefore, name and postal address of subscriber; Haverinen, para 252***)**

the telephone number associated with a subscriber (*the home GSM network stores customer information, such as authentication codes and user identity; therefore, telephone number of subscriber; Haverinen, para 252*);

the existing Fully Qualified Domain Name for a subscriber **(***The NAI is in form of imsi@sonera.fi (for example "1234567@sonera.fi") or imsi@gsm.org (for example "1234567@gsm.org"); the NAI carries an identity (for example as text or as an identifier number) of the mobile telecommunications network whose subscriber the mobile node is and an identification of the domain of the mobile node; Haverinen, para 165*); and the status of any mobility services established earlier for a subscriber (*the MT needs first to send its IMSI to the MA with which it is registering. Then the MA is able to use the FAAA-HAAA protocol in order to obtain GSM authentication information for the MT (as described above) and use this information for generating the K, with the MT; Haverinen, para 199*).

Regarding claim 30, Haverinen discloses a stable forwarding agent of a mobile routing system for use in securely authenticating subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, where a first run of an authentication and key agreement procedure has been performed in the radio communication network between a mobile node and an authentication server of the radio communication network so as to authenticate the mobile node to the radio communication network (*authentication algorithms which are referred to as A3 and A8. These algorithms run on the SIM and in the GSM telecommunications network. These algorithms and a GSM shared secret K.sub.i*

are known by the SIM and the GSM telecommunications network operator, which typically stores them in an HLR (Home Location Register) of a Mobile services Switching Centre (MSC); In authentication, the GSM telecommunications network operator generates a challenge RAND (128 bits random code used as challenge) that is a 128 bit random code, which is to be used as a challenge, a corresponding 64 bit GSM session key Kc and a 32 bit signed response SRES for verifying the response to the challenge. The 64 bit session GSM session key Kc is generated by the A8 algorithm as A8(K.sub.i,RAND) and the 32 bit long SRES (signed response extension of the system) is generated by the A3(K.sub.i,RAND); the GSM telecommunications network operator sends the RAND to its subscriber (GSM telephone), the RAND is received by the subscriber and the subscriber passes it to the SIM, which reproduces SRES and Kc. Then the SIM responds to the challenge by sending the SRES. The operator receives the SRES and can confirm the identity of the SIM. The GSM telecommunications network operator can also verify that it shares a Kc with the SIM. Then the Kc can then be used to encrypt data traffic over a GSM radio channel. The advantage of this challenge-response mechanism is that Kc never need be sent over the GSM radio channel and thus it cannot be eavesdropped; therefore, the first run of authentication and key agreement procedure*; Haverinen, para 0169-0170; fig. 1 and para 0173*) , the stable forwarding agent comprising:

a relay (i.e. HA or FA, para 29 of applicant spec)for relaying messages associated with a second run of the authentication and key agreement procedure between the mobile node and the authentication node of a radio communication network, the second run resulting in generation of a shared secret (*The HAAA verifies that SIGNsres is valid by checking that the equation SIGNsres=HASH2(K,n*SRES) applies with the values the MT has received. The HAAA sends the result (whether the SIGNsres is valid) to the FAAA. If the SIGNsres is valid, the HAAA sends*

also the K (i.e. shared secret) to the FAAA; Authentication is complete and the FAAA and the MT share the K; Haverinen, para 186-187);

a receiver for receiving and using the shared secret to authenticate the mobile node, for collecting subscriber contact information from the authentication server, and for receiving a public key from the mobile node (*the home GSM network stores customer information, such as authentication codes and user identity; The MT sends to the FAAA a Network Access Identifier NAI and a protection code MT_RAND (also known in Mobile IP terminology as nonce) generated by the MT. The MT_RAND remains the same during an authentication session and it is meant to hinder replay attacks; Haverinen, para 252*);

a key determining processor for agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured (*The MT sends to the FAAA a Network Access Identifier NAI and a protection code MT_RAND (also known in Mobile IP terminology as nonce) generated by the MT. The MT_RAND remains the same during an authentication session and it is meant to hinder replay attacks; Haverinen, para 178*; *a secure channel is formed between the PAC and the GAGW using their previously arranged shared secret; Haverinen, para 270*); and

a mobility service provisioning processor for using the subscriber contact information to assign a suitable Fully Qualified Domain Name and/or IP address to said mobile node and for updating a subscriber database and DNS server with the Fully Qualified Domain name and/or IP address and the public key provided by the mobile node (*The NAI is in form of imsi@sonera.fi (for example "1234567@sonera.fi") or imsi@gsm.org (for example "1234567@gsm.org"); the NAI carries an identity (for example as text or as an identifier number) of the mobile telecommunications network whose subscriber the mobile node is and an identification of the*

domain of the mobile node; Haverinen, para 165; Authentication is complete and the FAAA and the MT share the K; the FAAA is functionally connected to several HAAAs and the FAAA selects the correct HAAA based on the domain part of the user's NAI, for example "sonera.fi"; the FAAA is configured to communicate with a single HAAA and always sends the message in step 1 to that HAAA; the MA can create/update the security context for the MT; Haverinen, para 0187-0193)

Although Haverinen discloses all of the limitations, Haverinen fails to expressly teach updating a subscriber database and DNS server with the Fully Qualified Domain name and/or IP address. However, the preceding limitation is known in the art and is taught by the Ju reference. Ju teaches a method for accessing a packet data service through an Internet service network by a mobile station having a unique domain name, the method comprises allocating an IP address for the packet data service to the mobile station; storing the domain name and the allocated IP address matched to the domain name in a DNS server; and providing the packet data service to the mobile station using the IP address matched to the domain name (Ju, para 00013). Therefore, it would have been obvious to one of ordinary skill in the art to modify Haverinen mobility server by including the DNS server in order to store an IP address allocated to the mobile station and a domain name granted to the mobile station by the AAA during accounting set up process of data session for packet service to a mobile station as taught by Ju.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHHEAN THAO whose telephone number is (571)270-7497.

The examiner can normally be reached on Monday-Friday 8:00 am-5:30pm; off every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dwayne Bost can be reached on 571-272-7023. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Dwayne D. Bost/
Supervisory Patent Examiner,
Art Unit 2617

/CHHEAN THAO/

Examiner, Art Unit 2617